Submission on PDPC's Public Consultation on Approaches to Managing Personal Data in the Digital Economy

Company:	MSIG Insurance (Singapore) Pte. Ltd.
Address:	4 Shenton Way #21-01 SGX Centre 2 Singapore 068807
Contact Person:	Ms Looi Pek Hong
Tel:	6827 2400
Email:	pekhong_looi@sg.msig-asia.com

No	Question from PDPC	Response from MSIG Insurance
Question 1	Should the PDPA provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent?	While we generally agree with this proposal, we would like clarification from PDPC that this does not remove the need for express consent for marketing messages via telephone calls and SMS.
Question 2	Should the proposed Notification of Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., impractical to obtain consent and not expected to have any adverse impact on the individual)?	The proposed condition "not expected to have any adverse impact" is subject to interpretation and will need further clarification or revision. While an organisation may view something as minimal impact, an individual may view the same thing as important or significant. The purpose of notification is to inform all customers, including those who are on Do Not Call list. Customers will not be aware of any notification if it allows individuals to opt out of notifications. Further, what form should the risk and impact assessment take? Is PDPC going to prescribe a minimal standard of assessment, or are organisations free to develop their own assessment?
Question 3	Should the PDPA provide for Legal and Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification?	Yes, but in what form should the risk and impact assessment take? Will this be of retrospective effect? Will there be a cut-off date for the personal data that can be used for this purpose?
Question 4	Should the proposed Legal or Business Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., not desirable or appropriate to obtain consent and benefits to the public clearly outweigh any adverse impact or risks to the individual)?	We ask for further clarification on what constitutes "Legal or Business Purpose". "Business" appears to be rather broad and vague. Does "Legal" mean that a legal action in a court of law must be anticipated or commenced? There is already currently an exception on "investigation". What is the difference between this and the proposed "Legal or Business Purpose"? Guides on examples of what constitutes "Legal or Business Purpose" would be welcomed.

		In what form should the risk and impact assessment take?
Question 5	What are your views on the proposed criteria for data breach notification to affected individuals and to PDPC? Specifically, what are your views on the proposed number of affected individuals (i.e., 500 or more) for a data breach to be considered of a significant scale to be notified to PDPC?	We generally support this proposal but for a data breach to be considered of a significant scale to be notified to PDPC, we propose that this be expressed as a percentage of the data in possession as opposed to a numerical figure (as 500 could be easily breached or not breached depending on the size of data in possession). Separately, we need to define clearly what constitutes as a breach that "does not pose harm to affected individuals". Does Birthday greetings/rewards letters that only state the "month of birth" constitute such a breach? Is customers' NRIC number on its own sensitive data? What about name and address?
Question 6	What are your views on the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectoral regulations?	Preferably, only one set of notification should suffice. PDPC may consider working with other regulatory bodies governing specific sectors to align the notification requirement. E.g. for a Suspicious Transaction Reporting, organisations only need to electronically file the STR report with the CAD, and the Monetary Authority of Singapore is automatically notified. Further, does PDPC expect to be notified of penalties or disciplinary actions taken against specific organisations by their sector regulatory bodies?